SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

A. Management Safeguards (Cont'd).

9. Annual Filing of Certificate of Compliance. On an annual basis, a corporate officer of the Company will sign and file with the Federal Communications Commission (FCC) a Compliance Certificate (Appendix 1) stating his or her personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules. A statement will accompany the Certificate explaining how the Company's operating procedures ensure that it is or is not in compliance with the FCC's CPNI rules, as well as an explanation of any actions taken against data brokers and a summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI. Additionally, the Company must report on any information it has with respect to the processes pretexters are using to attempt to access CPNI, and what steps it is taking to protect CPNI. This annual filing will be made with the FCC's Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

   a. The "actions against data brokers" discussed above refers to proceedings instituted or petitions filed by the Company at either at a state or federal commission, or the court system.

   b. The "summary of all Customer complaints received" refers to number of Customer complaints the Company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

10. The Company will review these procedures on a continuing basis to ensure compliance with all FCC regulations, and will revise these procedures as needed to reflect any subsequent revisions to the applicable rules and regulations addressing CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

B. Recordkeeping.

1. The Company will maintain records of its own sales and marketing campaigns that use CPNI in files clearly identified as such. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

2. The Company will maintain records of its Affiliates' sales and marketing campaigns that use CPNI in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

3. The Company will maintain records of all instances where it discloses or provides CPNI to third parties, or where third parties are allowed access to CPNI, in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

4. The Company's policy is to maintain records of Customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

5. The Company will maintain separate files in which it will retain any court orders respecting CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards.

1. The Company must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.

2. The Company must properly authenticate a Customer using a method appropriate for the information sought prior to disclosing CPNI based on Customer-initiated telephone contact, online account access, or an in-store visit.

   a. Telephone Access to CPNI containing Call Detail Information (CDI). The Company will only disclose Call Detail Information over the telephone, based on Customer-initiated telephone contact, if the Customer first provides the Carrier with a password, as described in Section 10.C.3., that is not prompted by the Carrier asking for Readily Available Biographical Information, or Account Information. If the Customer does not provide a password, or does not wish to create a password, the Company may only disclose Call Detail Information by sending it to the Customer's Address of Record, by calling the Customer at the Telephone Number of Record (rather than using Caller ID), or by providing it in person upon presentation of a Valid Photo ID matching the Customer's Account Information.

   - If the Customer is able to provide Call Detail Information to the Company during a Customer-initiated call without the Company's assistance, then the Telecommunications Carrier is permitted to discuss the Call Detail Information, provided by the Customer (but not other Call Detail Information).

   - If a Customer requests non-Call Detail Information CPNI, the Company need not first obtain a password from the Customer, but must nevertheless authenticate the Customer.

   - The Company need not require Customer to setup a password, but must provide the Customer the option to do so.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

b. Online Access to CPNI. The Company must authenticate a Customer without the use of Readily Available Biographical Information, or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. Once authenticated, the Customer may only obtain online access to CPNI related to a Telecommunications Service account through a password, as described in Section 10.C.3., that is not prompted by the Company asking for Readily Available Biographical Information, or Account Information.

- The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

c. In-Office Access to CPNI. The Company may disclose CPNI (including Call Detail Information) to a Customer who, in the Company's office, first presents a Valid Photo ID matching the Customer's Account Information.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

3. Establishment of a Password. In order to provide a Customer CPNI containing Call Detail Information, the Company must authenticate the Customer without the use of Readily Available Biographical Information, or Account Information. The Company may establish passwords, among other methods:

   a. At the time of service initiation;

   b. Using a Personal Identification Number (PIN). The Company may supply the Customer with a randomly-generated PIN, not based on Readily Available Biographical Information, or Account Information, which the Customer would then provide to the Carrier prior to establishing a password. The Company may supply the PIN to the Customer by a Company-originated voicemail or text message to the Telephone Number of Record, or by sending it to an Address of Record so as to reasonably ensure that it is delivered to the intended party.

   c. The Company is not required to create new passwords for customers who already have a password, even if the password uses Readily Available Biographical Information. However, the Company must not prompt the Customer for Readily Available Biographical Information, and any back-up authentication method cannot use Readily Available Biographical Information.

4. Establishment of Back-up Authentication Methods. The Company may create a back-up Customer authentication method in the event of a lost or forgotten password. The back-up Customer authentication method may not prompt the Customer for Readily Available Biographical Information, or Account Information. The shared secret is the preferred method for establishing backup authentication.

5. Reauthentication. If a Customer cannot provide the correct password or the correct response for the back-up Customer authentication method, the Customer must establish a new password.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

6. Notification of Account Changes. The Company must notify a Customer immediately whenever an authentication password, Customer response to a back-up means of authentication for lost or forgotten passwords, online account, or Address of Record is created or changed.

   a. This notification is not required when the Customer initiates service, including the selection of a password at service initiation.

   b. This notification may be through a Company-originated voicemail or text message to the Telephone Number of Record (not caller ID), or by mail to the Address of Record, and must not reveal the changed information or be sent to the new Account Information.

   c. A change of address should be mailed to the former address, rather than the new address.

7. Business Customer Exemption. The Company may bind itself contractually to authentication regimes other than those described in this Manual for services they provide to business Customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches.

1. The Company will take reasonable steps to protect CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.

2. The Company must notify law enforcement of a Breach of its Customers' CPNI. A Breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

3. The Company shall not notify its Customers or disclose the Breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement. As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the Breach, the Company shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni. The Company will indicate its desire to notify its Customer or class of Customers immediately concurrent with its notice to the USSS and FBI.

   a. Notwithstanding any state law to the contrary, the Company shall not notify Customers or disclose the Breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in the following Paragraphs b. and c.

   b. If the Company believes that there is an extraordinarily urgent need to notify any class of affected Customers sooner than otherwise allowed under Paragraph a. immediately above, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected Customers only after consultation with the relevant investigating agency. The Company shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such Customer notification.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches (Cont'd).

c. If the relevant investigating agency determines that public disclosure or notice to Customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the Company not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the Company when it appears that public disclosure or notice to affected Customers will no longer impede or compromise a criminal investigation or national security. The agency will provide in writing its initial direction to the Company, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by Carriers.

4. After the Company has completed the process of notifying law enforcement as described in Paragraphs 3.a – 3.c. above, it shall notify Customers of the Breach.

5. Recordkeeping. The Company must maintain a record, electronically or in some other manner, of any Breaches discovered, notifications made to the USSS and the FBI pursuant to the above paragraphs, and notifications made to Customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the Breach, and the circumstances of the Breach. The Company must retain the record for a minimum of 2 years.

APPENDIX 1

ANNUAL CERTIFICATE OF COMPLIANCE WITH CPNI RULES

Including—

FILING INSTRUCTIONS AND ACCOMPANYING COVER LETTER TO THE FCC

Filing Instructions

Attached is a model Certificate of Compliance with the FCC's CPNI rules. It contains blanks for the insertion of Company-specific information. **The certificate must be signed by an officer (i.e., the President, V.P., Secretary) of the Company. Electronic copies of the Certificate and cover letter may be obtained from the Telecommunications Association of Michigan.**

The FCC's revised CPNI rules state that a carrier must file a "compliance certificate" each year that addresses compliance with the FCC's CPNI regulations, along with:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with the FCC's CPNI regulations;
- An explanation of any actions taken against data brokers; and
- A summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI.

The attached Certificate of Compliance addresses these subjects in a single document. Also attached is a sample cover letter to accompany the filing.

This Certificate of Compliance must be filed on or by March 1 each year relating to the prior calendar year.

Simply filing the certificate is not enough. Your Company must make sure that it actually engages in the practices discussed in the Certificate before signing and filing it.

Below are the procedures for filing. **Electronic filing is recommended unless the Certificate contains confidential information on the Company's method of combating pretexting (See Paragraph 16 of the Certificate; consultation with legal counsel is advisable).** Mailed filings are not deemed to be filed until actually received from the FCC (47 CFR 1.7). Thus, paper filings should be mailed several days before they are due.

ELECTRONIC PAPERLESS FILING:

The easiest way to file is electronically through the FCC's Electronic Comment Filing System (ECFS): http://www.fcc.gov/cgb/ecfs/. Put both the cover letter and Certificate in a single PDF. Click on "Submit a Filing" on the right side of the screen. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and the proceeding number which is 06-36. Under "Document Type," select "Statement."

Additional electronic copies must go to: Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, **byron.mccoy@fcc.gov;** and Best Copy and Printing, Inc. (BCPI), **fcc@bcpiweb.com**.

PAPER FILING:

Companies that choose to file by paper must file an original and four copies of each filing. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554.

Companies can also send their filings using commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail), by sending them to 9300 East Hampton Drive, Capitol Heights, MD 20743.

Additional paper copies must go to: Byron McCoy, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, Room 4-A234, 445 12th Street, S.W., Washington, D.C. 20554, or by email to byron.mccoy@fcc.gov; and Best Copy and Printing, Inc. (BCPI), Portals II, 445 12th Street, S.W., Room CY-B402, Washington, D.C. 20554, (202) 488-5300, or via e-mail to fcc@bcpiweb.com.

[Company Letterhead]

EB Docket No. 06-36

February 4, 2011

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S.W., Suite TW-A325
Washington, D.C. 20554

RE: **Form 499 Filer ID #802095**

Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached the Company's Annual Compliance Certificate for the previous calendar year, 2010. The Compliance Certificate includes the Company's:

- Statement explaining how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,

Todd Roesler
Chief Executive Officer
Ace Telephone Association

Enclosure

cc: Byron McCoy, Telecommunications Consumers Division, FCC Enforcement Bureau, byron.mccoy@fcc.gov

Best Copy and Printing, Inc., fcc@bcpiweb.com

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Including:

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

Explanation of Any Actions Against Data Brokers, and

Summary of all Customer Complaints Received

Todd Roesler signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of Ace Telephone Association (Company), related to the previous calendar year, 2010.

This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

On Behalf Of The Company, I Certify As Follows:

1. I am the Chief Executive Officer of the Company, and therefore an officer of the Company. My business address is 207 E Cedar Street, Houston MN 55943.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to CPNI.

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

3. I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's regulations governing CPNI, including those adopted on March 13, 2007 in CC Docket No. 96-115.

4. The Company ensures that it is in compliance with the FCC's CPNI regulations. The Company trains its personnel regarding when they are authorized to use CPNI, when they are not authorized to use CPNI, and how to safeguard CPNI. The Company maintains a CPNI Compliance Manual in its offices for purposes of training of new and current employees, and as a reference guide for all CPNI issues. Our CPNI Compliance Manual is updated to account for changes in law, including the FCC's most

recent changes to its regulations governing CPNI, adopted on March 13, 2007 in CC Docket No. 96-115. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company complies with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters."

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has not encountered any circumstances requiring it to take any action against a data broker during the year to which this Certificate pertains.

Summary of all Customer Complaints Received

15. The following is a summary of all customer complaints received during the calendar year of 2008 concerning the unauthorized release of CPNI: None.

16. The Company has no knowledge of any attempt by pre-texters to access its Customer's CPNI.

Date: _____

_____

Todd Roesler
Chief Executive Officer
Ace Telephone Association

APPENDIX 2

EMPLOYEE VERIFICATION OF CPNI MANUAL REVIEW

Employee Verification

Employee Name: _____

I have reviewed the Company's Customer Proprietary Network Information Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

_____
Employee Signature

_____
Date

c: personnel file
CPNI file

Return to Human Resources Department

APPENDIX 3

SAMPLE OPT-OUT NOTICE

OPT-OUT NOTICE

Important notice about your account

Federal law allows telephone companies and wireless telecommunications carriers to use, disclose, or permit access to your information as required by law; with your approval; or in providing the service from which your information was obtained.

What is this information?
It is information called Customer Proprietary Network Information (CPNI) and includes the phone numbers called by a consumer, the frequency, duration, and timing of such calls, and any services purchased by the consumer, such as call waiting.

Who can use this information?
Ace Communications Group and Ace Link Telecommunications, Inc. will use this information. However, we will not provide your personal information to unaffiliated third parties for the marketing of third-party products without your consent.

How can Ace use this information?
This information can be used to advise you about innovative communications services or new communications technology and products. We also provide this information to third parties in order to provide certain Ace-offered products and services, such as our long distance service through Onvoy.

Will Ace protect my information?
YES! You have the right, and we have the duty, under federal law, to protect the confidentiality of this information. Therefore, regardless of whether or not you consent to allowing us to continue providing you with marketing and educational mailings, your account information will be treated confidentially.

How does Ace protect my long distance call information?
If you or someone else calls us with questions about your call details, we will only give out the information by:

[1] calling the person back at the phone number listed on the account, or

[2] mailing the information to the billing address on file, or

[3] asking the person for the password that you had already set up for your Ace account. *(The password cannot be something familiar to others such as Social Security numbers, mother's maiden name, birth dates, etc.)*

What action is necessary on my part to show consent?
No action is necessary. If you do not contact us within 30 days and indicate that we may not use the information to continue providing you with marketing and educational mailings, we will continue to do so.

What if I do not consent?
You can contact us using the contact information below and indicate that you are withdrawing your approval of our use of your CPNI. We will not accept verbal requests; they must be written or emailed. After we receive your request, you will not receive targeted marketing information from us.

Denial of approval will not affect the provision of any services to which you subscribe. You may miss the opportunity to learn of new, innovative service proposals, new packaging that could reduce your monthly bill, or new lower rates on services such as long distance. You will still receive monthly bill inserts, quarterly newsletters, and other publications that are sent to all customers at the same time to keep you up to date on what is happening at Ace.

If I consent, can I change my mind?
YES. You can contact us at any time. Until you do so, your consent is valid.

Contact information:
Ace Communications Group.
PO Box 360
Houston, MN 55943
email: info@acegroup.cc

[Note to Company: Please consult Section 7.E. of CPNI Compliance Manual for when Opt-Out Notices are permissible.]

APPENDIX 4

SAMPLE FORM FOR DISCLOSURE OF CPNI TO THIRD PARTY ON CUSTOMER'S REQUEST

ACE Communications Group

ACELink Telecommunications, Inc.

Authorization Form

Current customer name: _____

Address: _____

City/state/zip: _____

Customer number or telephone number(s): _____

I am the customer of Ace Communications Group or Ace Link Telecommunications, Inc. (Ace) for telecommunications services under the account identified above and request and authorize Ace to disclose to the Authorized Person(s) identified below, upon request by the Authorized Person, all details regarding my account to which I have access, and to make changes to my account.

I agree this authorization will remain valid until Ace receives written notice from me revoking or changing the authorization.

Current customer signature (*must be notarized*): _____

Date: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

(*Add Remove*) Authorized Person: _____ Contact number: _____

4-digit password must be created: _____ _____ _____ _____

(Authorized Person(s) will need to know this password to access the account.)

To be completed by Notary Public

Subscribed and affirmed before me in the County of _____, State of _____, this _____ day of _____, 20____.

_____
Notary's official signature

_____
Commission expiration date

APPENDIX 5

Log of Customer Complaints Related to CPNI

LOG OF CUSTOMER COMPLAINTS RELATED TO CPNI

Affected Customer Name	Date of Complaint	Description of Complaint

APPENDIX 6

Section 222 of the Communications Act

Available upon request from Administration

APPENDIX 7

FCC CPNI Rules

Available upon request from Administration

Red Flags Compliance Manual and Operating Procedures

For

Ace Telephone Association
Ace Telephone Company of Michigan, Inc.
Ace Link Telecommunications, Inc.
Allendale Telephone Company
Drenthe Telephone and Communications

February 4, 2011